KuppingerCole Report

WHITEPAPER

By Mike Small
October 07, 2021

Securing your IaaS Cloud

While the major CSPs (Cloud Service Providers) go to great lengths to secure the services that they provide it is up to the client of the Cloud service provider to secure their use of these services. The responsibility for security and compliance is shared. This report describes the approach that clients (or in other words tenants) of Cloud infrastructure need to take to ensure that they use IaaS services in a way that is secure and compliant, including examples of how to realize this with Amazon Web Services. In our recent independent 2021 "Kuppinger Cole Market Compass report on Global IaaS Providers Tenant Security Controls", AWS was evaluated as an outstanding provider. This report also contains an extract of our evaluation of AWS from the Market Compass report.

By **Mike Small**
sm@kuppingercole.com

Content

1 Introduction / Executive Summary

The cloud has established itself as an important enabler of digital transformation. It has changed the way organizations do business and the events of 2020 have dramatically accelerated this digital transformation. Retailers had to increase their online presence, manufacturers had to reorganize their shop floors and employees worked remotely for large stretches of time to name just a few examples. This was only made possible by the way in which cloud services provide the ability to respond rapidly to changing business needs. The cloud has now become an integral part of business-critical operations where security and compliance are essential considerations.

The major CSPs (Cloud Service Providers) go to great lengths to secure the cloud infrastructure underneath the services that they provide but it is up to the cloud clients (or Cloud Infrastructure tenants) to secure the way they use them. When companies use the cloud, they must ensure that they meet their responsibilities and verify that the CSP meets theirs. Many of the security related incidents around the use of cloud services that have been reported result from failures by the cloud client to meet these responsibilities.

This report describes common security related business risks that can arise from the use of cloud services and covers the approach that cloud clients should take to mitigate these risks. Some of the risks that can be mitigated with the right strategy include using backups to protect data, preventing public access to sensitive data, and removing well-known technical vulnerabilities that can be exploited in cyber-attacks. It also provides examples of the support and building blocks that Amazon Web Services offers to help their clients to achieve this. In our 2021 independent "Market Compass report for Global IaaS Providers Tenant Security Controls", Kuppinger Cole ranked AWS as an outstanding vendor for the range of the security capabilities it provides to help its clients run their cloud workloads. An excerpt of the AWS profile from the Market Compass report can be found at the end of the document.

Most organizations now have a hybrid IT environment. The best approach to meeting the security and compliance challenges of this is good governance with a consistent approach to the security of IT services regardless of how they are delivered. When using the Public Cloud, the responsibilities for security and compliance are shared between the cloud client and the CSP. The client does not manage or control the underlying cloud infrastructure but is responsible for managing everything above the service provided. The client is also responsible for compliance with laws and regulations governing the processing of data.

Governance sets measurable business-related objectives for IT services and monitors how well these objectives are being met. This approach allows the organization using the IT service to focus on their business and the service providers to focus on delivering the required service.

This governance-based approach to the use of a cloud service means that clients of the cloud must clearly set out their business, security, and compliance objectives for the service. This provides benefits that stretch beyond governance and compliance.

2 Highlights

- This report focusses on the steps an organization needs to take to manage common business risks when using an IaaS cloud.
- These risks include loss of business continuity, data breaches, and regulatory compliance failure.
- Identity and access governance are a foundational element of cloud security and compliance.
- It describes the best practices that cloud clients should adopt such as:
  - Identify critical data and protect it in transit, at rest and during processing using encryption or pseudonymization.
  - Most cyber-attacks exploit well known technical vulnerabilities - implement automated processes to identify common vulnerabilities within your cloud elements.
  - Have a backup plan - plan for how you would manage in the event that your data or the cloud service becomes unavailable.
  - Take a zero-trust approach to network security - set up logically isolated segmentation of your resources within your virtual cloud network.
  - Support for compliance - make sure that the service supports your compliance obligations.
  - Use what is provided - the services, templates, and tools that the service provides.
  - Look for AI based tools to support your secure use of the cloud service.
  - Trust but Verify - verify that the security and compliance of any cloud service that you use meets your security and compliance obligations.

3 Why you need to Secure your use of Cloud

The Coronavirus epidemic forced organizations to change the way that they do business. Retailers have had to move online, manufacturers have had to reorganize their shop floors, and employees have had to work from home. In response to this organizations have accelerated their digital transformation by several years in a matter of months. This was only made possible by the way in which cloud services provide the ability to respond rapidly to changing business needs. However, when IT services are used for business-critical applications, security and compliance become essential considerations. While organizations understand how the service that they deliver themselves meets their security and compliance obligations they are often less sure how these will be met when using a cloud service.

The major business risks from the use of IT services, however they are delivered, are loss of business continuity due to downtime caused by IT service failures as well as cyber-attacks such as ransomware and denial of service; data breaches including data leakage as well as unauthorized access; and the failure to comply with obligations imposed by laws or regulations. The organization must take appropriate steps to mitigate these risks when they use cloud services just as they would for other IT service models.

Compliance failure - organizations are faced with a wide and increasing number of laws and regulations relating to the processing of data. These include the EU GDPR (General Data Protection Regulations), CCPA (California Consumer Privacy Act), financial services regulations such as PCI-DSS as well as export regulations, intellectual property laws and others around the world. An organization needs to ensure that they meet their compliance obligations when using cloud services.

Business continuity - cloud services provide strong capabilities to ensure IT services remain operational, but clients of cloud services are not immune to the impact of errors, cyber-attacks, component failures and natural disasters. A recent fire at a data centre in France is an example of this risk. The use of the cloud service depends upon the end-to-end availability of resources which include the multiple networks, systems at the edge and end user devices. Organizations must include all of these in their business continuity plans.

Data breaches and fraud - the network and the cloud service infrastructure are outside of the direct control of the cloud clients and so their data is potentially at risk while in transit, during storage, and while being processed. There are also concerns that the CSP may gain unauthorised access to the cloud clients' data or be subject to legally binding requests for this data from a government.

These risks are not unique to the use of cloud services but there are several factors which increase when using cloud. Firstly, cloud services are frequently used for internet facing applications and this increases their exposure to various forms of cyber-attacks. Secondly, cloud clients sometimes fail to properly manage their responsibilities for security and compliance. Finally, many fail to adapt and apply their normal internal security and compliance controls, such as identity and access governance and vulnerability management, to their use of cloud services.

While major CSPs (Cloud Service Providers) like AWS go to great lengths to secure the services that they provide it is up to the clients of cloud providers to secure how they use cloud services. The responsibility for security and compliance is shared between the cloud client and the CSP. The client does not manage or control the underlying cloud infrastructure but is responsible for managing everything above the service provided. The client also remains responsible for compliance with laws and regulations governing the processing of data. AWS clients can also choose to involve AWS Managed Services or work with an AWS Managed Service Provider Partners. AWS Managed Service Provider Partners provide clients full lifecycle solutions in cloud infrastructure and application migration. They offer support in key areas such as planning and design of their cloud infrastructure as well as with cloud migration and operation.

4 Securing your Cloud

Good governance, with a consistent approach to the security of IT services regardless of how they are delivered, is the best approach to the hybrid IT environment that most organizations now have. This sets measurable business-related objectives for IT services and then monitors that these objectives are met. This approach allows the organization using the IT services to focus on their business and the service providers to focus on delivering the required service.

A governance-based approach to the use of a cloud service means that the client must clearly set out their business, security, and compliance objectives for the service.

Figure 1 illustrates the responsibilities of an IaaS tenant (or cloud client) within the context of an overall security governance fabric. This fabric should cover all of the elements that need to be secured to ensure a consistent and cost-effective approach. It should provide a common set of services that use appropriate tools to achieve the business defined security and compliance objectives.

There are several existing frameworks for the governance of and the best practices for IT security management. For example, the NIST Cybersecurity Framework (CSF) focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The ISO 27000 series of standards provides best practice recommendations for the management of information risks through security controls. There are also other industry-specific frameworks such as the PCI-DSS (Payment Card Industry Data Security Standard). Organizations should adopt the appropriate elements of these frameworks and apply them consistently across all of the IT services that they use. This report will revisit this topic later and includes examples for how AWS technology provides support for the areas shown in this illustration.

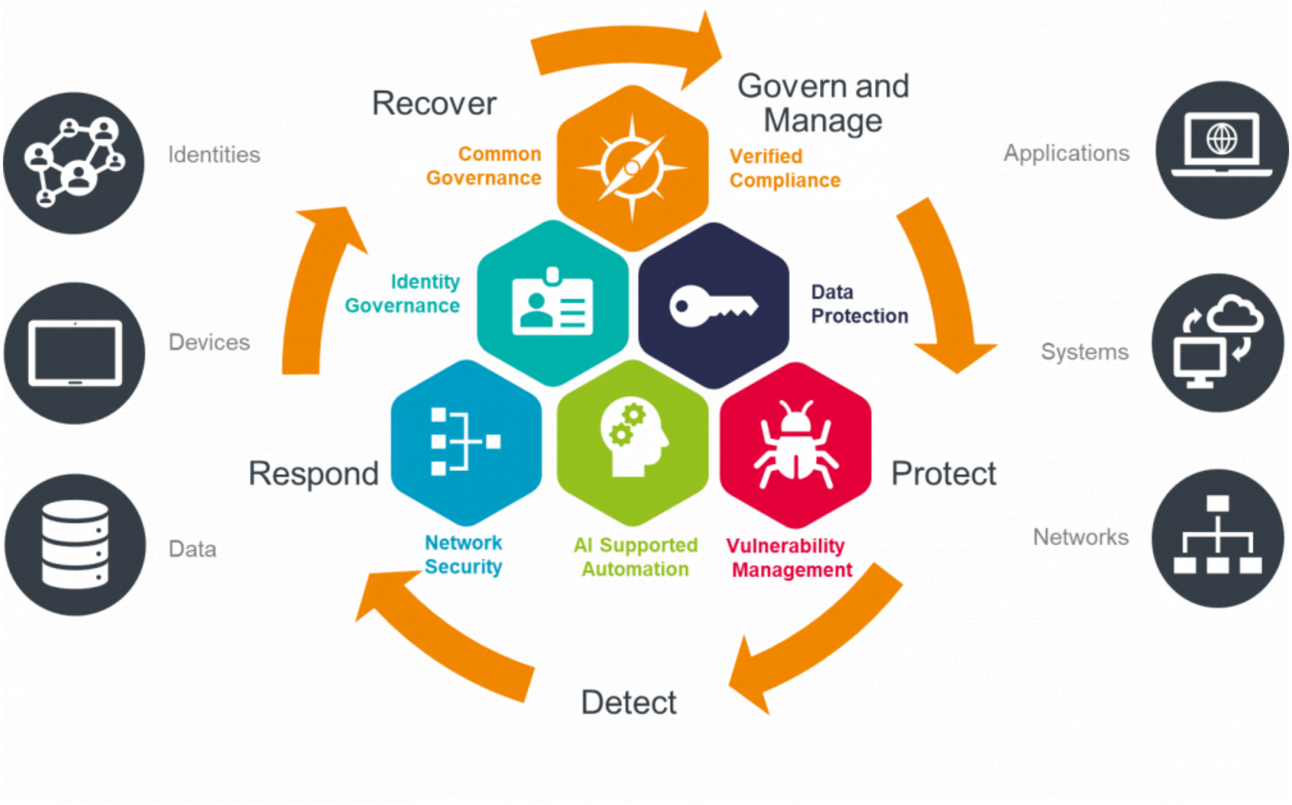


Figure 1: A Fabric for Cloud Security Governance

4.1 Understand your Responsibilities as a Cloud Client

Most of the reported cloud related cyber incidents have been due to errors by the cloud client (or in other words cloud tenant).

The CSP is responsible for the security of the services that they deliver, and the client of the CSP is responsible for securing the way in which they use these services. The client is always responsible for securing access to their data and their services. Make sure you understand your responsibilities and that you fulfil them. How responsibilities are shared is illustrated in Figure 2.

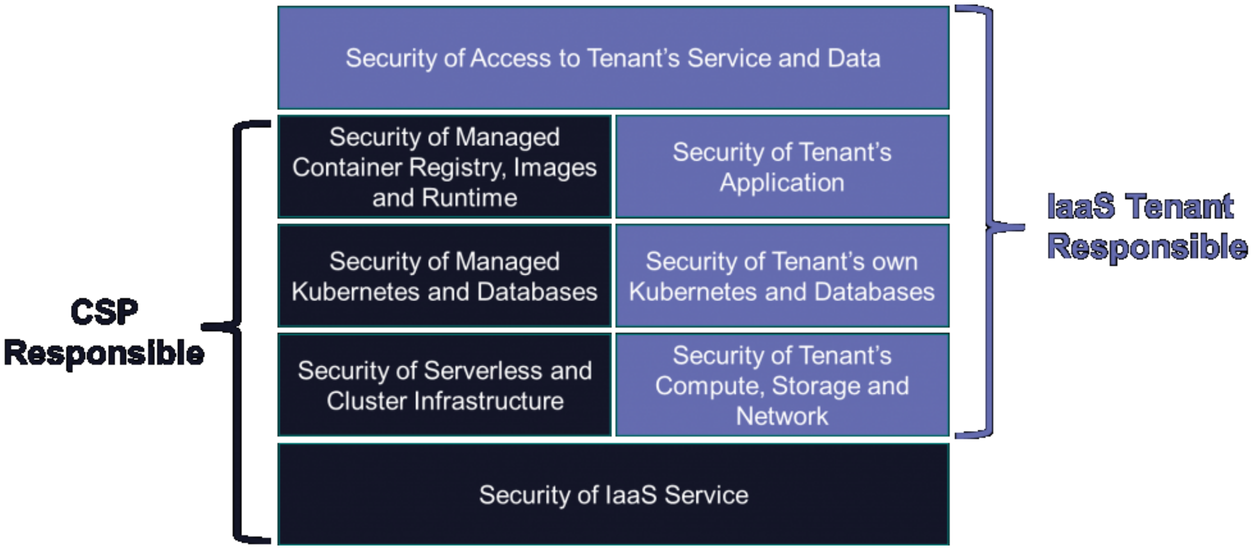

Security of Access to Tenant's Service and Data
Security of Managed Container Registry, Images and Runtime
Security of Tenant's Application
Security of Managed Kubernetes and Databases
Security of Tenant's own Kubernetes and Databases
Security of Serverless and Cluster Infrastructure
Security of Tenant's Compute, Storage and Network
Security of IaaS Service
CSP Responsible
IaaS Tenant Responsible

Figure 2: Responsibility for security

For basic IaaS services, such as compute, network, and storage, the CSP is responsible for securing the infrastructure used to provide the service up to the hypervisor. The CSP has no control over how these are used by its client. The client is responsible for security for everything above the hypervisor.

For platform services the CSP is responsible for the security of these services up to the client's interfaces. These include serverless computing, the infrastructure used for container services and orchestration, as well as middleware such as DBaaS.

For example: For compute services such as an Amazon EC2 instance, clients are responsible for the management of the guest operating system (including updates and security patches), any application software or utilities they have installed on the instance, plus the configuration of the AWS-provided firewall (called a security group). For abstracted services, such as the storage service Amazon S3, AWS operates and is responsible for the infrastructure layer, the operating system, and platforms which clients use to store and retrieve data. Customers are responsible for securing their data (including encryption options), classifying their assets, and using IAM tools to apply the appropriate permissions.

4.2 Identity and Access Governance

Your cloud administrative access rights are a prime target of cyber adversaries - make sure that you protect them.

The client is always responsible for managing their access to the service and the security of their data. This makes identity and access governance a foundational element of cloud security and compliance. It is especially important to control access by the client's administrators - these privileged access rights are a prime target of cyber adversaries since they potentially provide access to all of the client's cloud assets.

Because of this risk, the organizations using the cloud must actively govern the whole lifecycle of these privileged access rights. The organization should integrate cloud access governance with their existing identity management processes for employees and associates. Since these usually result in the identities and entitlements being held in a corporate directory such as Microsoft Active Directory this is an important integration point. The client should use this as the master source of identity and entitlements for cloud access using standards such as ADFS or SAML.

Access rights should be based on the principle of least privilege with enforced segregation of duties: cloud administrators should only be granted access to the services and resources for which they are responsible. This is especially important in large organizations where the cloud service may be used by several lines of business. Cloud clients should also regularly conduct reviews to identify excessive or abnormal access rights as well as orphan accounts (i.e., accounts without an owner). These reviews should include the entitlements of service elements as well as people.

The service should provide tools to support these processes such as RBAC (Role Based Access Controls) and PBAC (Policy Based Access Control) with policy templates. Support for strong authentication is essential to minimise the opportunity for cyber attackers to use stolen credentials to gain access. Where the service provides APIs, these should be authenticated and subject to similar controls. The activities of the service administrators at a cloud client should be logged so that abnormal access patterns can be detected using UEBA (User and Entity Behaviour Analytics).

For example, AWS clients can use the AWS Control Tower service which provides an easy way to set up and govern a secure, multi-account AWS environment, which AWS calls a landing zone. AWS Control Tower creates the client's landing zone using AWS Organizations, bringing ongoing account management and governance as well as implementing best practices based on AWS's experience working with thousands of clients as they move to the cloud. With AWS Control Tower, builders can provision new AWS accounts in a few clicks knowing that their accounts conform to organization-wide policies. The setup employs blueprints, which capture AWS best practices for configuring AWS security and management services. AWS Control Tower also provides sets of rules, called guardrails, which help enforce security policies or detect violations.

"Prior to using Control Tower, we needed to manually separate data in our production system between different accounts. By using Control Tower, we were able to eliminate these time-consuming, inconsistent tasks. As a result, we could ensure central auditability across all accounts and make sure that specific guardrails are in place, such as restricting our Amazon S3 buckets from becoming public. We now have faster account setups, increased security by using standardized guardrails, and better compliance due to central audit logs."

Hendrik Nehnes, CTO - Regis24

Regis24 is a global provider of consumer credit data and related data science services. With 50+ employees, and 14 million Euros of revenue generated in 2019, the independent, full-service provider delivers reliable, business-relevant information on private persons to support companies in maintaining updated customer records. Regis24 implemented AWS Control Tower to gain central auditability of their AWS infrastructure and central security across all accounts.

4.3 Data Protection

Your business-critical data could be at risk from cyber-attacks, ransomware, and misuse as well as system failures. Make sure that you protect it.

The confidentiality, integrity, and availability of the client's data can be compromised while it is in transit, stored, and being processed. In addition, accidents, cyber-attacks, service element failures and natural disasters can lead to data becoming lost or inaccessible with consequential loss of business continuity. The cloud client must evaluate these risks and take appropriate steps to mitigate their impact.

Data flowing to and from the cloud service as well as within the service itself can be intercepted. To ensure its confidentiality it is essential to encrypt data in transit using the most up to date technology such as TLS 1.2 or 1.3 or IPSEC VPN. This is necessary both for data flows within the in-cloud network as well as over public networks.

The data stored within the service could potentially be compromised in several ways.

- The media containing the data may be lost or discarded at the end of its life.
- The area on the physical media containing the data may be reallocated to another client without the data being erased.
- The CSP's staff may gain access to the data while performing their legitimate activities.
- The CSP may be subject to a legal request from a government to hand over the client's data.

To protect against these risks, the client should classify their data held in the service and encrypt sensitive and regulated data using certified strong encryption algorithms. Clients should retain control over the encryption keys. The service should give each client full control over encryption of their keys. The client should also consider the CSP's controls to prevent access to client data while performing legitimate infrastructure administration.

In order to process data, it is usually necessary to decrypt it - this puts the confidentiality of that data at risk since there are tools available to extract data from processor memory as well as from machine snapshots.

The use cases below include the need to protect data while it is being processed. Where the use case demands it, the service should support one or more approaches to confidential computing, which protects data against unauthorised access during processing, such as:

- Trusted Execution Environment - where the data is only decrypted within a hardware protected environment. AWS supports this via AWS Nitro Enclaves which enable clients to create isolated compute environments to further protect and securely process highly sensitive data.

- Pseudonymization - the data is transformed so that the data in protected fields cannot be related to its real value without the use of extra data that is retained by the tenant.
- Homomorphic encryption - a form of encryption that allows the encrypted data to be processed without it being decrypted. However, this may only support a limited set of processing functions and may involve a high processing overhead.

There are various circumstances that could lead to the client being unable to access the applications and data held in the service. The data may be accidentally deleted, it may become corrupted due to application errors, ransomware, or localized failure. The client is responsible to ensure that their data is protected against these risks using backup and restore processes and the service should provide tools to help with that. The CSP should also provide capabilities to enable continuity of the client's service when individual service elements fail or become unavailable, and the client should use these capabilities where needed.

Depending on the region where an AWS client operates, additional regulations might apply. Where the cloud is used to process personal data of European Union residents, the cloud client must comply with the EU's General Data Protection Regulation (GDPR). This covers individuals' fundamental right to privacy and the protection of their personal data. In this context, the European Data Protection Board recently recommended additional technical measures that organizations must apply for GDPR compliance when EU personal data is transferred to a "Third Country" - in effect outside of the EU.

AWS provides online resources to help clients more easily complete data transfer assessments and to comply with the GDPR, taking into account the European Data Protection Board (EDPB) recommendations which are described in the link above in more detail. These resources also assist AWS clients in other countries to understand whether their use of AWS services involves a data transfer.

4.4 Technical Vulnerability Management

Most cyber-attacks exploit well known technical vulnerabilities - implement automated processes to identify and remove common vulnerabilities.

There are many documented technical vulnerabilities that cyber adversaries can exploit to disrupt IT services. The CSP is responsible for managing the vulnerabilities within the infrastructure supporting the services that they provide. However, the client is responsible for managing the technical vulnerabilities within their use of these services. The IaaS provider should offer the client capabilities to prevent, identify, and manage these.

The client should implement processes to identify common vulnerabilities - usually by regularly scanning their environment using automated tools. They should have a process to take appropriate action when vulnerabilities are identified. Since new vulnerabilities are constantly being discovered the client should also regularly update their software in the service.

Many vulnerabilities are caused by misconfiguration, and these can be avoided by implementing best practices. The client should configure their IaaS service elements according to best practices. The service should provide best practice templates and defaults as well as the capabilities to scan for deviations.

The client is responsible for the applications that they host in an IaaS service. Cyber-attacks frequently exploit application-level vulnerabilities, and it is up to the client to manage these. This could be through code scanning as well as dynamic testing. The service should support secure application development and testing.

A common error is that the cloud services by default sets external public access rights on data held within the service. The Cloud Service Provider should ensure that public access rights are not the default and provide the capability to scan for and remediate public access rights. For example AWS includes the "Amazon S3 Public Access Feature" that provides the ability for system administrators to block existing public access and to ensure that public access is not granted to newly created items.

4.5 Network Security Management

The network provides a route for cyber adversaries to attack your systems - take a zero-trust approach to network security.

Internet access could provide a route for cyber adversaries to gain access into the client's cloud service and then into their back-end systems. The CSP is responsible for securing the service network infrastructure against internet based cyber-attacks and the client is responsible for securing their service elements. The Cloud Provider should offer the client capabilities such as network firewalls and the client should configure these appropriately. The service should also provide capabilities to protect the client against large scale attacks such as DDoS (distributed Denial of Service).

Bruce Hellman, CEO at uMotif and AWS client comments: "Building on Amazon Web Services (AWS) allows uMotif's platform to easily scale from studies of a few dozen patients to research with tens of thousands of participants, with wide geographical coverage and millions of data points. uMotif's AWS infrastructure enables quick deployment of compute capacity when traffic increases and allows for integration with other solutions in the eClinical ecosystem. API endpoints are protected using AWS Web Application Firewall (AWS WAF), blocking out viruses and malicious attacks. Global hosting and language translation tools, an easy-to-use interface, and cloud infrastructure mean that uMotif's platform can be deployed anywhere, providing complete benefits to users. Using AWS allows us to deploy fast and scale quickly when traffic increases and enables us to configure and deploy studies consistently and securely. Working in life sciences, it's critical that our platform is secure and audit-ready at any time."

Using AWS, uMotif facilitates medical research by improving the quality of data captured during clinical *studies. The company's software makes it easy for patients to record their experiences during a study, using mobile devices like tablets and smartphones. The data is then regularly synced to a cloud-based, backend infrastructure running on the AWS Cloud.*

Kuppinger Cole recommends that the client adopts a "Zero Trust" approach to network security. This involves not only identifying the people but also the devices accessing individual service elements. One objective of a Zero Trust approach is to prevent so called lateral flow attacks where the cyber adversary can exploit access gained to one element within the cloud to connect to other elements as well as the client's internal systems.

To counter this, the client should segment their virtual cloud network to logically isolate their cloud resources. They should place their backend systems such as databases and applications servers that do not need internet access in private subnets. The client should also implement application-level traffic filtering using a WAF (Web Access Firewall) to prevent application level cyber-attacks such as SQL Injection.

Zero Trust, as well as TLS, involves the use of certificates to identify devices and to manage the encryption of network traffic. The client is responsible for managing these certificates and this can be a major task especially where large numbers of IoT devices are involved. The service should provide support for the client to securely manage these certificates.

The CSP should also provide capabilities for the client to identify and manage anomalous network traffic. This could be through cloud native capabilities or integration with the client's existing SIEM (Security Information and Event Management) processes and tools.

4.6 Service Management

Adapt your existing service and security management processes to include your use of cloud services.

Managing and administering the cloud service is an important consideration. Most organizations will already have existing IT management processes and tools. The client should carefully consider how to integrate the management and security of the cloud service into these.

Many organizations are already using a software defined IT environment, such as VMware, that is also supported by cloud vendors. Where organizations are already using this, it makes sense to extend its use into the cloud to provide a common management experience. However, this approach may sacrifice some of the service optimizations that are only available from the native cloud management tools.

Cloud clients should look for a policy-based service management approach that makes it easy for them to define, implement and enforce standards. This could be provided through service templates or predefined default policies.

4.7 Compliance Management

Make sure that the cloud is independently verified and use the capabilities provided to ensure that you use the service in a way that complies with your obligations.

Organizations must comply with a wide range of laws and regulations governing how the data they hold is processed and stored. The client must carefully consider how the use of cloud services will support their obligations under these. There are two aspects to consider - firstly whether the service itself complies with the relevant laws and regulations and secondly the support that the service provides to enable its compliant use.

Since the client has no control over how the infrastructure itself is managed, they must take a governance-based approach, setting clear and measurable objectives based on their compliance obligations and then verifying that the service meets these. The client must require evidence that the services they use comply with the laws and regulations that are relevant to their use case and that this evidence is accepted by the relevant regulator.

AWS Artifact Reports provide compliance reports from third-party auditors who have tested and verified compliance of the infrastructure run by AWS with a variety of global, regional, and industry specific security standards and regulations. AWS Artifact grants on-demand access to AWS' security and compliance reports and select online agreements. This includes for example Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals that validate the implementation and operating effectiveness of AWS security controls.

In addition, the service should provide the capabilities necessary for the client to comply with their own regulatory obligations. Since there is a wide range of laws and regulations the client must check that their individual needs will be met. The client should look for a CSP with predefined templates and assessment tools that cover the laws and regulations related to their use case.

Where the client itself has the responsibility to demonstrate compliance for their workloads run in AWS, AWS offers a service called AWS Audit Manager. AWS Audit Manager simplifies how AWS clients can assess risk and compliance with regulations and industry standards. Its prebuilt frameworks help translate evidence from cloud services into auditor-friendly reports by mapping a client's AWS resources to the requirements in industry standards or regulations, such as NIST 800-53 that we mentioned above, the General Data Protection Regulation (GDPR), as well as more industry-specific framework. This includes for example the Payment Card Industry Data Security Standard (PCI DSS) in the payments industry or the HIPAA (Health Insurance Portability and Accountability Act) and HITRUST (Health Information Trust Audience) frameworks in the healthcare sector.

AWS client Tangoe says: "At Tangoe, we have a large customer base in the Fortune 500 and government space that expects similar or better data protection standards compared to their internal policies. With that expectation comes regular audits and security assessments from customers and 3rd party independent firms. AWS Audit Manager helps immensely to streamline, simplify and in many cases, automate the evidence gathering."

Tangoe is a leading global provider of technology expense management and managed mobility services for enterprise.

Contractual agreements with special compliance-related clauses go some of the way toward providing the assurance needed. However, these should be supported by independent verification of the CSP's claims and, where necessary, technical controls that can be used by the client.

For example, one common regulatory obligation is for control over the geographic location where the client's data is held and processed. Sometimes this also includes the location and citizenship of the service administrators. The CSP should provide the client with technical controls over the location of their data backed by legal guarantees.

Some vendors offer a "cloud in a box" as a solution to these regulatory needs. This is either an appliance or hardware and software that can be installed and located wherever the client requires and under the direct control of the client. As well as supporting compliance needs, this also provides a consistent application environment and management experience.

AWS offers AWS Outposts which runs AWS infrastructure and services on premises, or wherever the client requires, providing a consistent hybrid experience. Furthermore, AWS Outposts enables clients to meet their data residency requirements, while benefitting from AWS services, even where there is no AWS Region.

The client should also consider the CSP's policies regarding disclosure of legal access requests to the client's data as well as policies relating to disclosure to clients of suspected and actual data breaches.

4.8 AI Support

Look for AI based support in the tools you use.

Machine Learning systems are ideally suited to the tasks of systems and security management where there are clear rules and well-defined environments. These technologies already form the basis for UEBA (User and Entity Behaviour Analytics), SIEM (Security Information and Event Management) as well as advanced authentication. These use AI techniques to identify abnormal patterns of behaviour from event logs and other sources. AI has also the potential to help the client to automatically patch, tune, and secure their cloud.

AWS offers several services that fall into this category: Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behaviour to protect AWS accounts, workloads, and data stored in Amazon S3 with the help of Machine Learning. A further example is Amazon Detective which makes it easy to analyse, investigate, and quickly identify the root cause of potential security issues or suspicious activities. Amazon Detective automatically collects log data from AWS resources and uses machine learning, statistical analysis, and graph theory to build a linked set of data that enables clients to easily conduct faster and more efficient security investigations.

Look at the level of automated support provided by the service to help the client to manage and secure their use of the service.

4.9 Security of the infrastructure

Trust but verify.

For IaaS, the CSP is responsible for the infrastructure and the managed services that their platform provides, and the client is responsible for everything else. The client must verify that the security and compliance of any cloud service that they use meets their security and compliance obligations within their risk appetite. The most practical approach for this is for the client to require that the service is independently verified as complying with the standards that are relevant to their use case. This verification should be part of the client's overall IT governance approach.

The client should evaluate the evidence that CSP provides **-** some important standards to look for are:

- ISO/IEC 27001:2013 provides a code of practice for information security management. This is fundamental to the delivery of a secure cloud service.
- ISO/IEC 27017:2015 provides additional controls to address cloud-specific information security threats and risks considerations.
- ISO/IEC 27018:2019 This document establishes commonly accepted guidelines for implementing measures to protect Personally Identifiable Information (PII) by provider of public cloud services.
- SOC reports conducted to SSAE 18 / ISAE 3402 provide independent attestations on a service provided by an organization including cloud services.
- The CSA STAR program includes a registry that documents the security controls provided by popular cloud computing offerings.
- CISPE Code of Conduct is a pan-European sector-specific code for cloud infrastructure service providers under Article 40 of the European Union's General Data Protection Regulation (GDPR)

5 Recommendations

Organizations need to take a business led approach to the use of cloud services. Will the use of a cloud service provide a better business outcome than one delivered by the organization itself? The answer to this question depends upon the specific business case. These recommendations cover the common concerns around security and compliance when using IaaS services. These need to be considered in the context of each prospective client organization's specific use cases.

Organizations are strongly advised to follow these best practices:

Good Governance with a consistent approach to the security of IT services, regardless of how they are delivered, is the best approach to the hybrid IT environment that most organizations now have. Governance sets measurable business-related objectives for IT services and then monitors that these objectives are being met. This approach allows the organization using the IT services to focus on their business and the service providers to focus on delivering the required services.

Understand your responsibilities. The responsibility for security and compliance of cloud services is shared between the client and the CSP. Most of the reported cloud related cyber incidents have been due to misconfigurations of the services by the client.

Manage Access. The client is always responsible for managing their access to the service and the security of their data. This makes identity and access governance a foundational element of cloud security and compliance. It is especially important to control access by the clients' administrators - these privileged access rights are a prime target of cyber adversaries since they potentially provide access to all of the client's cloud assets.

Protect your Data. Identify the data that is most important to your organization and make sure that you protect it. Encrypt data in transit using the latest technologies such as TLS 1.2 or above. TLS 1.3 is preferred and is becoming more commonplace. Encrypt data at rest and keep control over the encryption keys. Evaluate whether the risks to your data mean you also need to use confidential computing to protect it while it is being processed.

Have a Disaster Plan. Include the end-to-end infrastructure as well as the cloud service in your business continuity plan. Ensure that your data in the cloud is protected using backup and restore processes and tools. Use the capabilities provided by the service to ensure continuity of your service when individual service elements fail or become unavailable.

Remove Vulnerabilities. Most cyber-attacks exploit well known technical vulnerabilities. Implement automated processes to identify common vulnerabilities and to take appropriate action when vulnerabilities are identified. Keep the software elements up to date.

Take a zero-trust approach to network security. Segment your virtual cloud network to isolate resources.

Place backend systems such as databases and applications servers that do not need internet access in private subnets. Implement application-level traffic filtering using a WAF (Web Access Firewall) to prevent a range of application level cyber-attacks such as SQL Injection.

Use what is provided. Take advantage of the services, templates, and tools that the service provides to manage and use the service in a way that is secure and compliant with your needs.

Trust but Verify - verify that the security and compliance of any cloud service that you use meets your security and compliance obligations within your risk appetite. Require evidence that the service is independently verified as complying with the standards that are relevant to their use case.

6 Evaluation of AWS Tenant Security Controls

This is an excerpt from the 2021 Kuppinger Cole Market Compass report on Global IaaS Providers Tenant Security Controls.

The 2021 KuppingerCole Market Compass report on Global IaaS Providers Tenant Security Controls provides an overview of vendors and their product or service offerings in a certain market segment. This Market Compass focusses on Infrastructure as a Service (IaaS) from Cloud Service Providers (CSP) with a global presence and with a specific focus on the capabilities they provide for the tenant to ensure their secure and compliant use of the service.

6.1 Outstanding for Range of Tenant Security Capabilities: AWS

AWS provides a comprehensive range of capabilities out of the box for the tenant to use their service in a secure and compliant manner. Many of these capabilities are free and AWS provides predefined profiles and service defaults, which can be adapted by tenants, to help them to implement best practices. They cover not only access controls but also service element configurations as well as vulnerability detection and management. The AWS services include rich monitoring of all activities and events supported by event driven tools that can identify and alert on anomalies and detect services objects that are out of policy and trigger actions. AWS Audit Manager, recently released, enables internal and external IT auditors to demonstrate regulatory compliance or identify compliance issues based on this data.

OUTSTANDING FOR
SECURITY CAPABILITIES
GLOBAL IAAS PROVIDERS TENANT SECURITY CONTROLS
KUPPINGERCOLE ANALYSTS AG,
JUN 2021
MARKET COMPASS
2021

Figure 3: Outstanding for Range of Tenant Security Capabilities: AWS

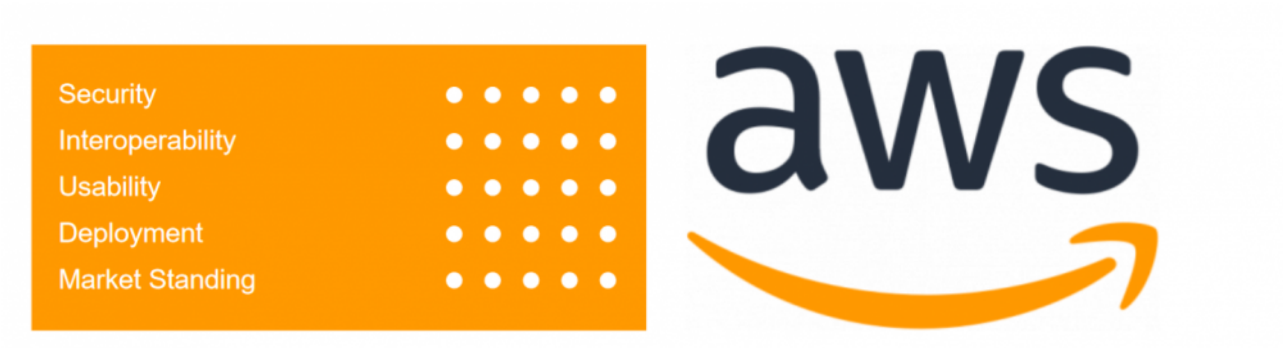
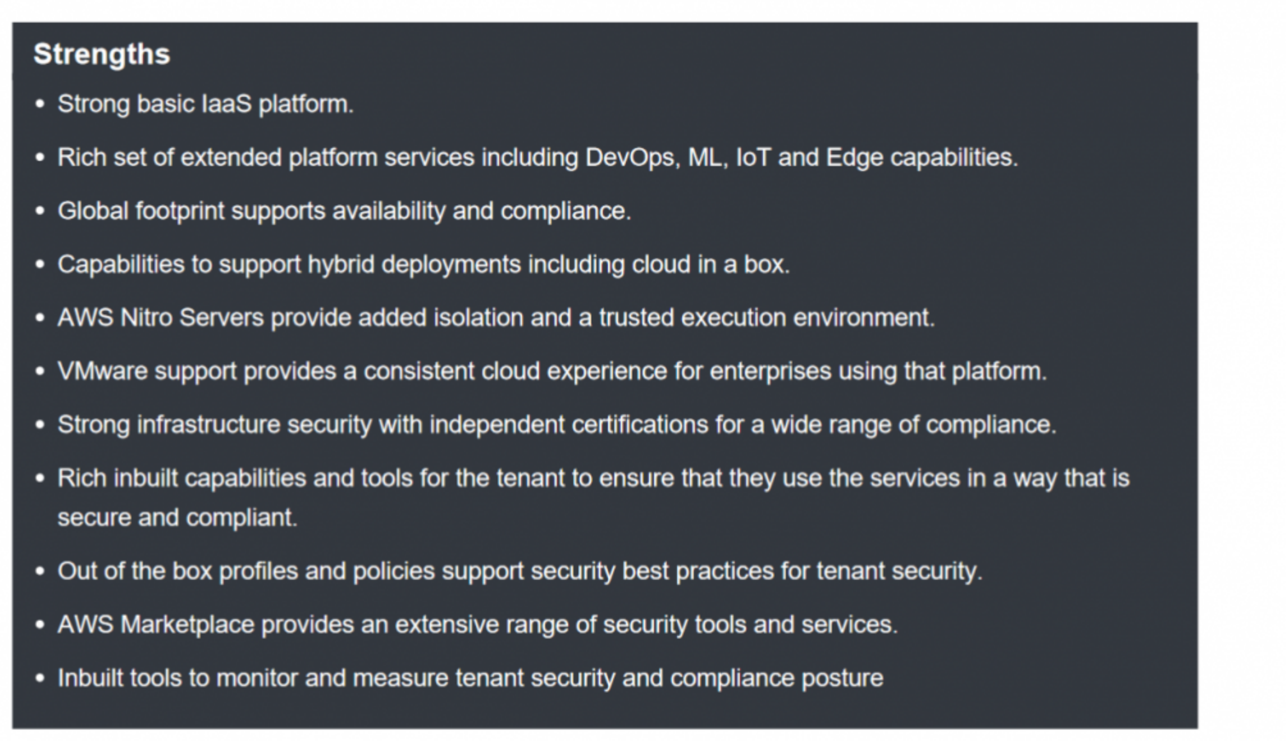


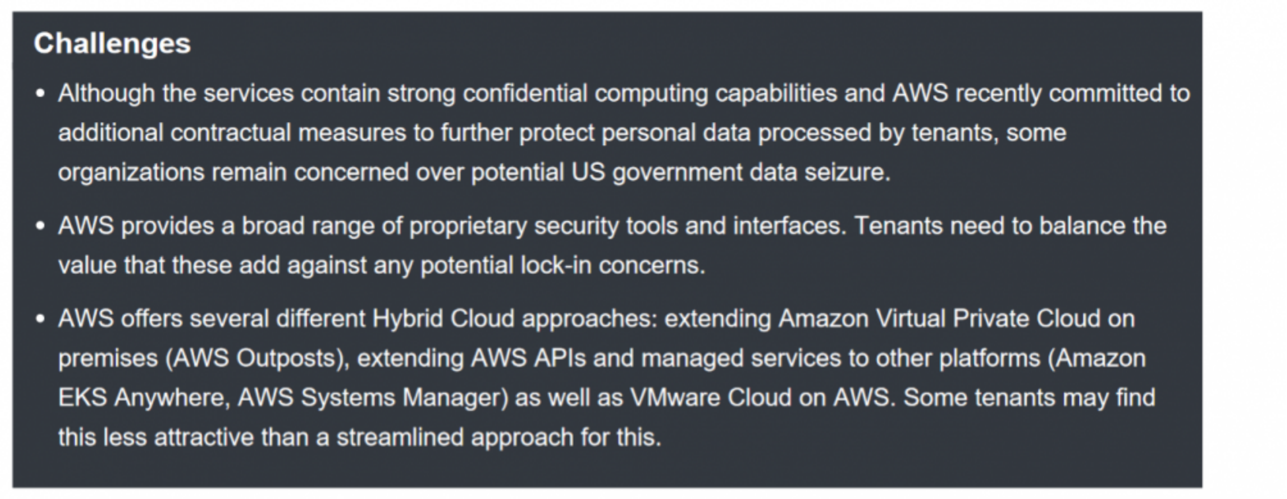
Figure 4: AWS Ratings



Strengths

- Strong basic IaaS platform.
- Rich set of extended platform services including DevOps, ML, IoT and Edge capabilities.
- Global footprint supports availability and compliance.
- Capabilities to support hybrid deployments including cloud in a box.
- AWS Nitro Servers provide added isolation and a trusted execution environment.
- VMware support provides a consistent cloud experience for enterprises using that platform.
- Strong infrastructure security with independent certifications for a wide range of compliance.
- Rich inbuilt capabilities and tools for the tenant to ensure that they use the services in a way that is secure and compliant.
- Out of the box profiles and policies support security best practices for tenant security.
- AWS Marketplace provides an extensive range of security tools and services.
- Inbuilt tools to monitor and measure tenant security and compliance posture

Figure 5: AWS Strengths



Challenges

- Although the services contain strong confidential computing capabilities and AWS recently committed to additional contractual measures to further protect personal data processed by tenants, some organizations remain concerned over potential US government data seizure.
- AWS provides a broad range of proprietary security tools and interfaces. Tenants need to balance the value that these add against any potential lock-in concerns.
- AWS offers several different Hybrid Cloud approaches: extending Amazon Virtual Private Cloud on premises (AWS Outposts), extending AWS APIs and managed services to other platforms (Amazon EKS Anywhere, AWS Systems Manager) as well as VMware Cloud on AWS. Some tenants may find this less attractive than a streamlined approach for this.

Figure 6: AWS Challenges

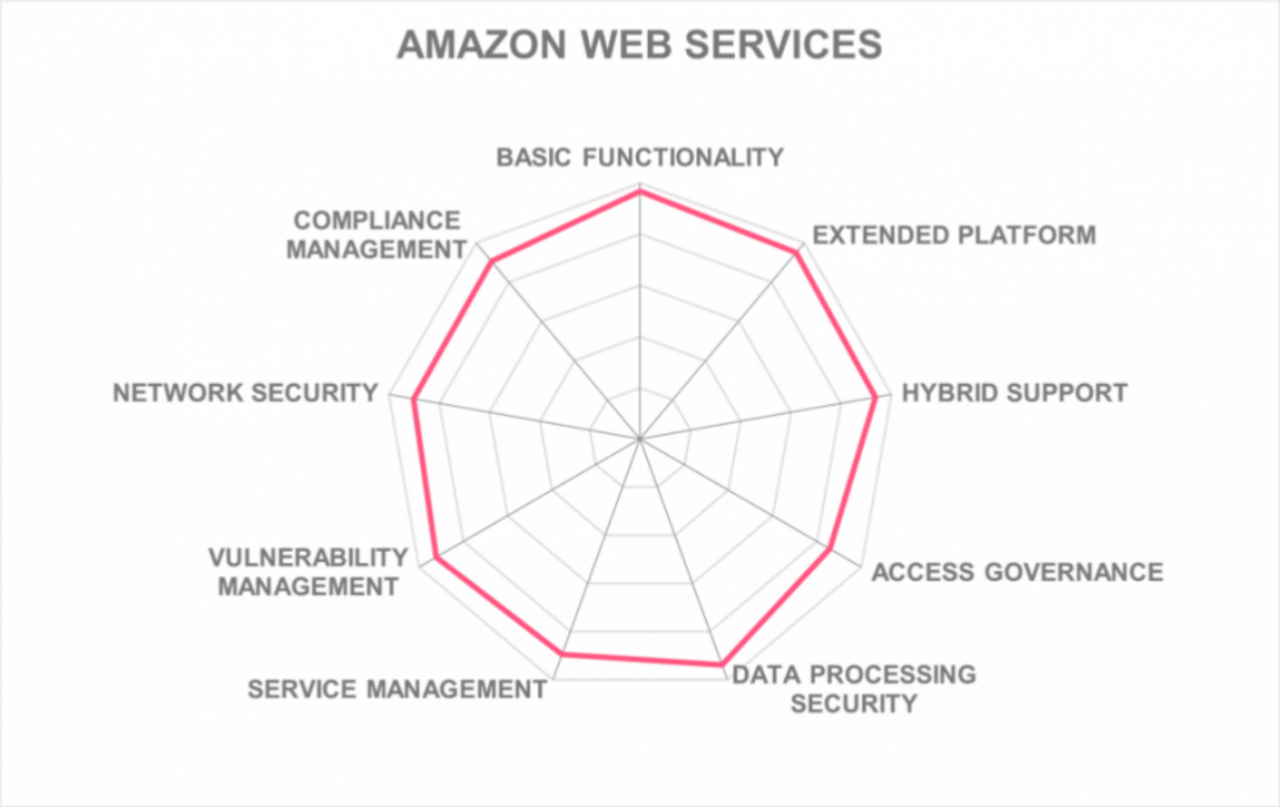


Figure 7: AWS Capabilities

7 Related Research

Buyers Compass: IaaS Tenant Security Controls - 80746

Market Compass: Global IaaS Providers Tenant Security Controls 80337

Architecture Blueprint: Hybrid Cloud Security - 72552

Advisory Note: Maturity Level Matrix for Cyber Security - 72555

Advisory Note: GRC Reference Architecture - 72582

Advisory Note: Protect Your Cloud Against Hacks and Industrial Espionage - 72570

Advisory Note: Security Organization Governance and the Cloud - 72564

Advisory Note: Cloud Services and Security - 72561

Advisory Note: How to Assure Cloud Services - 72563

Advisory Note: Firewalls Are Dead - How to Build a Resilient, Defendable Network - 72163

Architecture Blueprint: Access Governance and Privilege Management - 79045

Architecture Blueprint: Identity and Access Management - 72550

Content of Figures

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst ompany, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.